# Exploring Preliminary Challenges and Emerging Best Practices in the Use of Enterprise Blockchains Applications

Mary Lacity
Blockchain Center of Excellence
University of Arkansas
mlacity@walton.uark.edu

Shaji Khan
College of Business Administration
University of Missouri-Saint Louis
shajikhan@umsl.edu

## Abstract

*Enterprise blockchain applications can allow trading partners to transact directly without relying on trusted third parties and promise to: eliminate the need for reconciliations, instantly track and trace assets through a supply chain, provide unbeatable data provenance, settle transactions quickly and cheaply, and enable an information security model that is fault tolerant, resilient, and available. Many of these promised benefits seemingly address the challenges of non-blockchain based inter-organizational systems. However, this research indicates that blockchain based inter-organizational applications pose significant challenges of their own. Based on interview and participant observation data, we identified five challenges: (1) competing blockchain standards, (2) adjusting to different shared governance models, (3) intellectual property concerns (4) industrial espionage risks, and (5) regulatory uncertainty. We also identified emerging practices stakeholders are using to address those challenges when considering enterprise blockchain applications.*

## 1. Introduction

Use of blockchain technologies in the interorganizational enterprise applications context has garnered tremendous attention in the industry. Reports and opinions predict that blockchain based enterprise applications will revolutionize business and reshape the economy [3, 9, 12, 26]. Enterprises are interested in blockchain technologies because they promise a significant amount of business value by providing the ability to transact directly with trading partners without the use of trusted third parties, eliminating the need for reconciliations, instantly tracking and tracing assets, providing data provenance, settling transactions quickly and cheaply and enabling a resilient information security posture. Put simply, blockchain based applications promise to solve many types of issues (e.g., those related to technical aspects, governance, transparency, efficiency, transaction costs, provenance, information security, and so on.) surrounding existing interorganizational systems [9, 10].

Despite the explosion of interest, our prior research found that there were very few enterprise blockchains applications in production in 2017-2018 notwithstanding the billions of dollars in blockchain investments worldwide [12], the thousands of proofs-of-concepts across all industries, and the high-profile groups like R3, Hyperledger Project and Enterprise Ethereum Alliance working to facilitate enterprise adoption. A 4th quarter 2017 study of 200 blockchain projects by HfS, a research and consulting firm, corroborates our findings. HfS found that 90 to 95 percent of enterprises were still conceptualizing blockchains, conducting proof-of-concepts or piloting applications. Only 5 to 10 percent of pilots were progressing to production [8]. What's taking so long?

Indeed, while generally sharing the optimism, some have expressed concerns about the hype surrounding blockchain applications in business contexts [9] suggesting that significant issues must be overcome before the promise of blockchain technologies is realized. Others have argued that many of the issues surrounding existing interorganizational systems, such as interoperability concerns, will manifest within the blockchain contexts as well [23]. Yet others have compared blockchain technologies to the proverbial "hammer looking for the nails," arguing that many of the potential business applications blockchain is being tested for, do not need blockchains and existing institutions, applications etc. may be just enough [7].

Unfortunately, little is empirically known on just what challenges organizations are facing so as to shed light on the potential of blockchain technologies

URI: https://hdl.handle.net/10125/59904
ISBN: 978-0-9981331-2-6

in the enterprise context. There's even less empirical basis to determine what organizations are doing to address those challenges as they explore and develop blockchain applications.

This paper addresses this gap and contributes to the practice and research of interorganizational systems by empirically exploring the preliminary challenges organizations are facing in adoption of blockchain technologies and by identifying emerging best practices for addressing those challenges. We draw on data from a broader multi-year, mixed-method research program to specifically addresses the following questions:

- *What challenges to adoption of enterprise blockchain applications do enterprises face?*
- *What practices are enterprises using to address those challenges?*

Understanding these challenges and organizational practices to address them is important both from a practice perspective and from a theoretical perspective. To the extent organizations see potential for business value, we believe that a better understanding of challenges and best practices is crucial for any real progress. On the other hand, if indeed, there are significant issues that cannot be overcome in feasible ways then it is also important to take note. From a theory perspective, senior Information Systems (IS) scholars have often reminded us to pay attention to the Information Technology (IT) artifacts due to the crucial role they play in shaping organizations and societies [14, 22]. To the extent, one considers the very nature of blockchain technologies as fundamentally different than previous generations of technological innovations and to the extent that one appreciates the truly transformative and upending potential of blockchain technologies [24], it becomes imperative to better understand and study blockchain's evolution into the context of business applications.

The rest of this paper is organized as follows. To orient readers new to blockchain technologies, section 2 provides some background and overview of a blockchain application as an inter-organizational trading system. Section 3 briefly describes our research methods. Section 4 presents the findings related to five challenges and five emerging practices for addressing them. Section 4 provides discussion, limitations, and directions for future research.

## 2. Background

A blockchain application "is a distributed, peer-to-peer system for validating, time-stamping, and permanently storing transactions on a ***distributed ledger*** that uses ***cryptography*** to authenticate ***digital asset ownership*** and ***asset authenticity*** and ***consensus*** algorithms to add validated transactions to the ledger and to ensure the ongoing integrity of the ledger's complete history" [10]. Blockchain technologies are commonly associated with cryptocurrencies operating with a ***permissionless***[1] model. While enterprises are interested in the underlying technologies that drive these blockchains, they require more control in the form of ***permissioned***[2] blockchain applications. Moreover, a majority of potential enterprise use-cases of blockchain technologies revolve around inter-organizational systems.

In other words, by their very nature, enterprise blockchain applications involve a network of stakeholders (business networks, business-government-quasi-government networks, etc.) where the nature of the transactions as well as the standards and inter-organizational frameworks within which those transactions would be executed, need to be coordinated among the diverse stakeholders. Further, the technological standards and regulatory underpinnings must also be delineated.

### 2.1 A Blockchain Application as an Inter-organizational Trading System

A distributed blockchain application performs the vital functions of trusted third-parties (TTPs) by using computer algorithms and cryptography instead of relying on institutions to mitigate counter-party risks. Enterprises are interested in permissioned blockchain applications, which restrict access to authorized users and the rights or roles of those authorized users (see Figure 1).

Permissioned blockchains rely upon a front-end gatekeeper to enforce the rights of access. Unlike a trusted-third party that sits in the middle of transactions, the gatekeeper is like a security guard that checks a badge before allowing entry. It has no

[1] ***Permissionless*** blockchain applications like Bitcoin, Ethereum, and Stellar do not restrict access—anyone with access to the Internet may participate.

[2] ***Permissioned*** blockchain applications restrict access to pre-authorized users and will likely be built on protocols designed for enterprise adoption, such as Hyperledger Fabric, R3 Corda, Chain, Multichain, and Quorum discussed in this paper.

ability to alter the ledger or to stop smart contracts from executing.[3]

Transactions on the shared ledger are immutable, thus every party can be confident they are dealing with the same data. With one version of the truth transparent to all parties, there are no reconciliations, enabling faster settlement times and lower transaction costs.

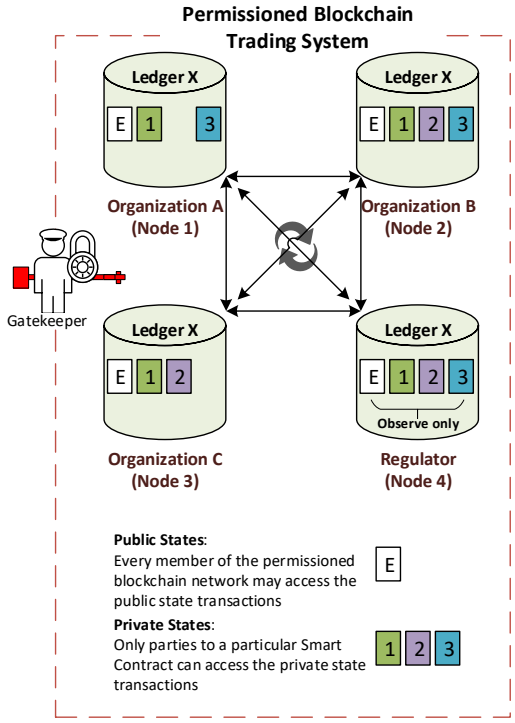


**Figure 1. Permissioned blockchain trading system with three trading partners, one regulator and no TTP. Organization A is party to smart contracts 1 and 3 but cannot observe smart contract 2; Organization B is party to smart contracts 1, 2, and 3; Organization C is party to smart contracts 1 and 2 but cannot observe smart contract 3; The regulator in this example is granted observation only access to all transactions.**

Use of cryptography-based identity and authentication in conjunction with immutability further enhances assurances of authorized access and data integrity. Permissioned blockchains can also use ***smart contracts***[4] to nuance roles within a blockchain application. Particular parties may play different roles within different smart contracts, such as observe, transact, validate, and add transactions to the ledger. For example, a permissioned blockchain may use smart contracts to create multiple, separate mini-ledgers as depicted in Figure 1.

Blockchain applications also promise heightened availability (a key security objective). Blockchain applications still function properly even if a high percentage of nodes are faulty—or even malicious—enabling resiliency and 100 percent availability. In theory, the only way to break a blockchain application is to commandeer more than 50 percent of the nodes before any of the other nodes notice.

In summary, the potential relative advantages of blockchain applications compared to trading systems that rely on TTPs are:

- The ability to transact directly
- No need for reconciliations
- Instant tract and trace of assets
- Reliable data provenance
- Control over one's own identity
- Faster settlement times
- Lower transaction costs
- Reduced threat of opportunism because agreements execute automatically
- Heightened security that is fault tolerant, redundant, and available

Despite the immense promised value, our research and industry reports suggest that adoption is still in nascent stages [8]. This slow pace has been attributed to technology immaturity and significant challenges that must be overcome. This paper focuses on identifying those challenges and emerging practices organizations are using to address them.

## 3. Research Methods

As mentioned above, this paper draws on a broader multi-year, mixed-method research program on use of blockchain technologies in enterprise contexts. In 2017, the lead author joined the Center for Information Systems Research, Massachusetts Institute of Technology as a Visiting Scholar to lead a research project on how enterprises were exploring blockchains. The research team included *Jeanne Ross*, Principal Research Scientist, and *Kate Moloney*, Research Specialist. In this paper, we report findings based on analyses of interview and

[3] This is true provided that the organization that serves as the gatekeeper operates fewer than 50 percent of the nodes; If a gatekeeper does operate 50 percent or more of the nodes, there is little point in using a blockchain except under specific circumstances, such as an intra-organizational blockchain across divisions and if concerns about organizational control are not an issue for the particular application.

[4] A smart contract is a piece of software that stores and then executes the terms of an agreement between parties.

participant observation data drawn from this broader research program.

### 3.1 Interviews

During interviews, we asked managers about their blockchain adoption journeys, their participation in blockchain ecosystems, and the practices and lessons they have learned so far. We asked research participants the following questions:

• How is the organization building blockchain capabilities? What strategies are being considered? Which applications are deemed to be the most promising, are already under development, or have been deployed?

• What challenges do organizations need to overcome to deploy blockchain applications into production? What are the key project and change management practices? How well have expectations been met so far? What are the preliminary outcomes and lessons learned?

As of this writing, confidential interviews were conducted with 38 key informants in 30 organizations. In order to minimize the potential for bias, we selected highly knowledgeable interview participants representing diverse perspectives, industries, and organizational characteristics [4]. We interviewed blockchain innovation leaders in large US national or global firms, including leaders from six global financial services firms, three global manufacturers, and two US healthcare providers. We have permission to specifically cite BNP Paribas, JP Morgan, Moog, and State Street as examples. We also interviewed blockchain heads in professional services firms, service providers, startups and nonprofit organizations. We conducted interviews in 19 such organizations, of which we have permission to cite Axiom, Blockchain of Things, Capgemini, Center for Supply Chain Studies, Cognizant, KPMG, LO3 Energy, and Stellar.

### 3.2 Participant Observation

The lead author also participated in the Center for Supply Chain Studies' project to define blockchain standards for tracing pharmaceuticals through the United States (U.S.) supply chain. The project examined ways the pharmaceutical industry can comply with the U.S. Drug Supply Chain Security Act (DSCSA) of 2013. The law requires that by year 2023 all parties in the U.S. supply chain must trace certain classes of pharmaceuticals from source to destination. *Bob Celeste*, Chief Executive Officer (CEO) and Founder of the Center for Supply Chain Studies, led the group of about 50 participants who represented pharmaceutical manufacturers, wholesalers, distributors, and retail and hospital pharmacies. The lead author was a participant in the event and took extensive notes aimed at capturing the key aspects of the issues and discussions. When possible, the lead author asked clarifying questions to other participants. This experience helped the lead author to better understand the perceived benefits, challenges, and concerns that supply chain partners have about shared blockchain applications.

### 3.3 Data Analysis

Interview and participant observation data were analyzed in an inductive and iterative fashion to help themes emerge and coalesce into 1) the major challenges in applying blockchain technologies for enterprise applications, and 2) the best practices indicated by the participants to help address those challenges. All interviews were recorded and transcribed into over 500 pages of text. Notes from participation observation were also analyzed. We followed a two-stage process. During the first stage of data analysis, we attempted to identify themes pertaining to organizational actions in exploring enterprise blockchain applications. The lead author read each interview and participant observation notes and coded the data to extract themes. Five major themes emerged from this process. When possible, details about specific blockchain technologies or consortia were compiled and written to supplement discussion of major themes by using those technologies or consortia as paradigmatic of the underlying theme. For example, when discussing a diversity of blockchain standards, we researched and presented four such major standards to highlight the issue.

During the second stage, we focused our attention on what participants identified as important best practices aimed at addressing each emergent challenge identified during the first-stage of analysis. When a particular best practice emerged, we explored the industry literature and our interview and participant observation data to identify instances of the emergent best practices or specific organizations employing them, to serve as exemplars in our research findings.

After the initial themes pertaining to challenges and best practices emerged, we next created written summaries (aimed at a practitioner audience). The summary write-ups were then sent to each participant who was quoted and the participant was requested to review their excerpt for accuracy. Participants made suggested revisions to improve clarity and precision. Separately, the lead author wrote a case study based

on participant observation data. This case study was then reviewed and edited based on input from the CEO of the case study site, Center for Supply Chain Studies. Each participant was asked whether they preferred to remain anonymous or to be identified. Fifteen participants granted permission to use their names and titles.

## 4. Findings

Our analyses revealed five major challenges that participants believe must be overcome before broader adoptions of blockchain technologies in enterprise contexts. Specifically, participants identified (1) competing blockchain standards, (2) adjusting to shared governance models, (3) intellectual property concerns (4) industrial espionage risks, and (5) regulatory uncertainty. We next explore each challenge and the emerging practices to address them.

### 4.1 Competing Blockchain Standards: The Race is Afoot

Our data suggest that a variety of different underlying blockchain standards are taking shape during the initial exploration of the use-cases as well as technological bases of blockchains. It appears that an assortment of industry alliances and consortia are competing in the standards arena.

"*The way we go about investing in blockchain is really multifaceted since nobody knows today which players will prevail…you cannot put all your eggs in one basket, so we have a very diversified approach with whom we work on the blockchain.*" — Jacques Levet, Head of Transaction Banking, EMEA at BNP Paribas

Blockchain standards are needed to specify rights of access and the rules for how transactions in a blockchain application will authenticate asset ownership and asset authenticity, how transactions will be structured, addressed, transmitted, routed, validated, sequenced, secured, and added to the permanent record. Standards will serve as the blueprints to ensure the integrity of records. As of year-end 2017, participants reported that many different groups are working on standards, but no one standard had emerged. Therefore, most of the research participants pursue the following practice:

#### Practice 1. Participate broadly in blockchain workgroups

As the following quote attests, most of our interviewees are participating in a number of blockchain working groups to define standards because they are not sure which working group will ultimately prevail:

"*So, from a strategy point of view, it's early days. We're probably in the situation that all the other big financial institutions are at the moment. Nobody's really backing one [consortium]. We're all trying to get to know as much about it as possible and see where it takes us. All we know is that it's going to be extremely disruptive.*" — IT Consultant and Architect for an Africa-based bank

Working groups, including consortia and non-profits, are defining blockchain standards and developing code bases and proof-of-concepts for business applications. As of August 2017, Deloitte identified 40 major consortia, of which 26 were focused on financial services, 10 were cross-sector, and three were in healthcare [6].

According to some of our research participants, large working groups may be the best bet for creating a *de facto* protocol in the long-run, but some are slow to agree upon standards. The value of smaller-sized working groups is that players can move faster; the downside risks are lack of wider adoption or eventual obsolescence if a new standard or platform emerges in the industry. Data suggests, many global firms mitigate the risk of backing the wrong horse by participating in both large and small working groups.

Enterprises in our study most commonly belonged to generic blockchain consortia, such as the Hyperledger Project and Enterprise Ethereum Alliance, as well as industry-focused consortia, such R3, B3i, and the Center for Supply Chain Studies (as mentioned above). For example, BNP Paribas participated in both large and small consortia and had invested in several FinTechs to influence, learn, and contribute to blockchain initiatives. A large consortium like R3 was very valuable because it brings many financial institutions into the conversation. Jacques Levet said, "*R3 is very useful because it's a way to organize discussions between the banks. Banks have historically not been very good at doing that on their own, so having a third party who organizes that is quite useful.*" BNP Paribas also joined two smaller consortia, with the goal that the banks will define standards and create a Request for Proposal (RFP) for FinTechs to develop the specified blockchain application [11].

While the main tasks of these working groups are to identify blockchain standards, build code bases, and/or proof-of-concepts, participants are also struggling with challenges about adjusting to different shared governance models, industrial espionage risks, adequate protection of joint intellectual property (IP) and regulatory uncertainty.

## 4.2 Adjusting to Shared Governance Models

"*Business agreements are the hardest things. We need to have rules of entry and play that protect consumers and protect the overall ecosystem. Getting people to play ball, that's the real tough thing.*" — Innovation Director for a US healthcare company

"*If the government had one iota how much fraud and abuse they could stop especially in pharmaceuticals, how they can purge the opioid thing, they would mandate blockchains tomorrow. It would be a mandated, you must participate on this within two years.*" — Head of Innovation for a US healthcare company

Both permissionless and permissioned blockchain applications rely upon shared governance models. No one entity should be able to unilaterally make decisions about changing the rules, upgrading the code base, or altering the immutable records or smart contracts.[5] Our participants identified several potential types of shared governance models at the level of a blockchain application, including democratic, representative, or regulatory. Each of these models have trade-offs.

### Practice 2. Carefully consider the trade-offs of shared governance models

With a **democratic** shared governance model, each participating member has an equal vote in deliberations. The members debate, deliberate and ultimately vote on proposed upgrades or fixes to address unexpected events like breaches or unintentional consequences from poorly crafted smart contracts. Open source communities that govern Bitcoin and Etherum are examples of democratic governance models. In those blockchain applications, miners vote on major decisions. The benefits of a democratic governance model are openness, which minimizes the threat of corruption, and power decentralization. The downsides are minority voices are muffled and decision-making can take a long time. When enough members disagree with the majority vote, hard forks in the blockchain can occur. Hard forks at Ethereum and Bitcoin are two prominent examples. Ethereum split into Ethereum and Ethereum Classic in June 2016 when the Ethereum community could not agree on how to handle an attack on a poorly worded smart contract; Bitcoin split into Bitcoin and Bitcoin Cash in August 2017 when the community could not agree on the proposed increase in block size. Their stories are important reminders of the implications of democratic governance. Specifically, ***an enterprise must be willing to defer to the community's will and live with the consequences of its majority rule.***

With a **representative** shared governance model, decision makers are elected or appointed to their roles. For example, a blockchain application in a pharmaceutical supply chain might have representatives from manufacturers, distributors, retail pharmacies and independent physicians who govern the application. This model will be able to make decisions quicker than a democratic one, but cabals may form where representatives collude. For example, manufacturers might vote as a group against the will of the retail pharmacies.

The governance might be relegated to a **regulatory** body. For example, participants in the Center for Supply Chain Studies envisioned that a regulatory body could allow any licensed pharmacies to participate in the shared blockchain application. In another context, one participant was helping a government with a blockchain application for passport control. The Passport Control Office would regulate and govern the application. The benefits are guaranteed regulatory compliance, but the model is centralized in that it places trust in one institution.

Overall, participants expressed concerns for any shared governance model. An enterprise may have a weighted vote in deliberations in proportion to their stake, but it will not be able to control them. This is a major mind-shift for many participants in our study.

## 4.3 Intellectual Property Concerns

"*Our industry is behind some other industries in our management of shared IP and our ability to collaborate and cooperate. We all jumped in to explore a use case and did some joint design thinking with two or three traditional competitors without thinking about who owns the intellectual capital that comes out the tail end of that workshop.*" — Innovation Lead for a global bank

Participants in our research expressed concerns about their working group's intellectual property rights. For example, a participant in the Center for Supply Chain Studies asked, *"How do we protect the intellectual property we've built as a team?"* The following practice emerged:

### Practice 3. Be sure to understand the working group's IP policy

Some consortia like the Hyperledger Project have visible IP policies, while others like R3 do not. For

[5] The only exceptions are under the circumstances in which an enterprise or a group of colluding enterprises operate at least 50 percent of the nodes.

example, Hyperledger's charter includes a clearly worded IP clause that in part reads:

"*Members agree that all new inbound code contributions to HLP (Hyperledger Project) shall be made under the Apache License, Version 2.0. All contributions shall be accompanied by a Developer Certificate of Origin sign-off that is submitted through a Governing Board and LF-approved contribution process. Such contribution process will include steps to also bind non-Member Contributors and, if not self-employed, their employer, to the licenses expressly granted in the Apache License, Version 2.0 with respect to such contribution…*

*Subject to available Project funds, HLP may engage The Linux Foundation to determine the availability of, and register, trademarks, service marks, and certification marks, which shall be owned by the LF* [27]."

R3's IP policies were not available to the public as of May 2017. An article by the *Business Insider* reported, "*Details about R3's share structure are not being disclosed, neither are details about the division of the intellectual property built atop the open-source Corda platform. However, Rutter (R3's CEO) did explain that while Corda itself is being open-sourced, the results of experiments conducted with partners within the R3 lab would be guarded more closely* [2]."

According to participants, some consortia required members to sign non-disclosure agreements, but only one reported that their working group required participants to sign IP agreements. One interviewee from a large bank explained, *"If you do highlight the need for some agreement [on shared IP], getting to common ground on what that agreement needs to look like and who should own the IP, it's sometimes weeks or even months in lead time. We as an industry need to work faster on those kind of repeatable processes."*

## 4.4 Industrial Espionage Risks

"*The issue is that some companies are afraid that information that's being collected for the blockchain will be used for other purposes. So, let's say I'm a pharmacy. If I verified all the products I have on hand, I'm announcing my inventory. Companies are concerned that this added intelligence could be used for other purposes such as contract negotiations, etc.*" — Bob Celeste, CEO and Founder of the Center for Supply Chain Studies

Participants expressed concerns about industrial espionage. With one shared ledger, how do enterprises prevent other entities from extracting meta-patterns about their inventory levels, customers, or suppliers etc.? Overall, participants believed technical solutions were the best ways to prevent industrial espionage:

### Practice 4. Design technical solutions to ensure confidentiality of data

Several technical solutions have been proposed. For example, many permissioned blockchains use smart contracts to restrict access to a particular agreement to the trading partners. Participants who are not party to a given smart contract agreement would not be able to interpret the transactions associated with that agreement on the ledger. Some permissioned blockchains, such as Ripple, allow private messaging, and some permissioned blockchains, such as Hyperledger Fabric, allow side channels. Using Quorum as an example, participants can execute private and public smart contracts so that the ledger is segmented into a private state database and a public state database [18]. Within a single ledger, all nodes can view Quorum's public states, but only those nodes party to private contracts can view private states. Such technical features did not alleviate all the participants' concerns because most enterprises will participate in multiple trading agreements and may be able to infer confidential data across smart contracts or side channels.

## 4.5 Regulatory Uncertainty

"*We don't know how the regulators are going to respond. At the end of the day, I think the early indications suggests that they're as intrigued by the value proposition associated with Blockchain as anybody. No regulator has come out of the gates telling you what you can and cannot do yet. That's a big unknown in our world.*" — Head of a blockchain Center of Excellence for a global financial services firm.

Regulators worldwide are examining the blockchain space. Some regulators are supportive, some are not, and still others have yet to deliberate. Many participants in this research wanted to educate regulators about blockchains, but at the same time, did not want regulators participating too closely in consortia lest their compliance weaknesses be exposed. Among the 30 enterprises we examined, LO3 Energy and Moog, Inc. were the most proactive about working with regulators. Both Lo3 Energy and Moog, Inc. serve as good examples of diverse organizations working actively with regulators. We briefly describe these organizations and how they are interfacing with regulators below to exemplify the below best practice.

### Practice 5: Actively work with regulators

**LO3 Energy.** LO3 Energy was founded by Lawrence Orsini in 2012 in Brooklyn New York with a vision to create a transactive energy platform that will allow neighbors to produce and consume locally produced electricity. The company is building a platform where producers sell excess energy capacity from their solar panels directly to neighbors. The platform comprises hardware, such as smart meters, switches, and controllers, and software embedded in the meters based on a proprietary blockchain-based application with a customizable, mobile user interface.

As LO3 continues to build and improve upon the platform, it is conducting live tests through a project called the Brooklyn Microgrid project. The Brooklyn Microgrid was running in a shadow market of 60 prosumers and over 500 consumers by year-end 2017. Live transactions would occur once required licenses from regulators were obtained.

Orsini has worked very closely with regulators since the company's launch. He's met with regulators from the US at both the State and Federal levels, as well with regulators from Australia and Europe [16]. He views his job as explaining the technology to help them understand what LO3's blockchain enables: a local, renewable, efficient "microgrid" that operates separately, but alongside, the utility grid. He hired lawyers who understood regulatory requirements. Orsini said: "*We've spent a fair amount of time and a decent amount of investment making sure that we can work within existing regulations. Lots of other people talking about doing something similar to us have never even considered how that impacts regulation. It takes a real strong team of regulatory attorneys to understand and be able to fit legally within the existing regulation [15]."* Orsini was among a minority of research participants who praised regulators for being receptive. He said, "*We have a very good relationship with the regulators. The regulators in New York are pretty excited about and engaged in what we're doing, particularly for the transactive energy platform [15]."*

**Moog, Inc.** Moog Inc. is a $2.5 billion US precision manufacturer and provider of integrated control systems. The blockchain adoption story begins in Moog's Transformative Technology division under Aircraft Controls. Colonel James Allen Regenor, Business Unit Director for Transformative Technologies, imagined the value of moving from centralized manufacturing to decentralized additive manufacturing, i.e., 3-D printing. He had flown fighter jets off of aircraft carriers, so he knew that when a part was not on board, the plane was grounded. Why not put a 3-D printer onboard a carrier?

The potential business value was enormous, such as significantly less downtime, lower inventory costs, lower customs fees, and lower shipping and transportation costs [25]. The challenges to realize such a decentralized manufacturing process—particularly in such a highly regulated context—were equally as enormous. Regenor explained, "*With 3-D printing, you have to worry about complex parts being counterfeit. Anybody can print something that looks like the part they are holding in their hand. It won't have the same material properties or the same characteristics, but the guy pulling it off the shelf will not know the difference [20]*."

Moog would need a decentralized network with the highest security. Regenor and his team realized that blockchain technologies might be the ideal technical solution [19]. Moog is now building a platform-based business model for the entire lifecycle of 3-D printed parts from part design to part decommissioning called VeriPart. Regenor was also an early advocate of getting regulations for verifying parts created by additive manufacturing. He needed the US government to create 3-D printing regulations for Department of Defense (DoD) acquisitions. Regenor took the current federal regulations for electronic parts and substituted the word "electronic" for "additive manufacturing" and brought it to legislators [19]. Moog also informed the US House Armed Services Committee about the threat of counterfeiting for additive manufactured parts. Legislators understood the concern; the National Defense Authorization Act of 2018 includes funds for additive manufacturing technology development and requires briefings on blockchain technologies from agencies [21].

## 5. Discussion, Limitations, and Implications for Future Research

"*Most of the organizations that we're speaking to are at an exploratory phase. Pretty much saying, 'we're trying to understand this'. Very few have really identified use cases that they're going to production scale and get a critical mass of partners on within the next six to ten months.*" —Practice Head for FS Analytics & Blockchain at a global consulting firm

"*We're definitely several years away from large applications. A few applications will be in production maybe in three years. But mass production won't likely be here for five years.*" — Nilesh Vaidya, SVP Head of Banking & Capital Market Solutions at Capgemini

Our study identified some challenges that need to be addressed before enterprises can deploy and scale blockchain applications across processes, industries and geographies. As indicated by the quotes above, solving these challenges will take time. Our paper contributed to practice by highlighting five approaches organizations are using to address those challenges.

However, an important limitation of this paper is that it does not include a discussion of technical challenges and efforts to address them. The technical underpinnings are indeed likely to play a significant role in the eventual business adoption and impacts of blockchain technologies. We hope future studies could include both technical and non-technical challenges in the study of blockchain adoptions and impacts. Despite this limitation, this study also has some important implications for research.

A long and robust stream of Information Systems literature has addressed various aspects of interorganizational systems [1, 13, 22]. Studies have examined the antecedents to adoption of interorganizational systems and their impacts on the governance of economic transactions. Yet others have studied the organizational impacts of adoption in terms of strategic, operational, and social aspects [22]. Within this broad literature, a variety of technologies underpinning interorganizational systems have been the subject study; from earlier studies on Electronic Data Interchange [5], to studies of both closed and open standards based technologies [22].

While our findings indicate some parallels with this broad literature, we believe that, broadly speaking, blockchain based IT artifacts [cf. 22] could indeed potentially alter both practice and research on interorganizational systems in fundamental ways. Some recent expositions argue that given the very nature of blockchain technologies (e.g., distributed ledger, transparency etc.) fundamentals notions such as trust, within and between organizations, and organizational structures could now be reexamined [e.g., 24]. Similarly, others [e.g., 17] argue that blockchain technologies enable new systems of value that require a new economic model.

Due to space limitations, we briefly discuss some important implications of our findings in relation to the literature on interorganizational systems. Our findings suggest an interesting set of developments related to competing standards and working groups/consortia for blockchain. Not only are organizations participating in multiple such groups due to the current flux and uncertainty in predicting dominant standard paradigms, they are also actively shaping those standards and tools that make adoption easier. While scholars have compared the evolution of blockchain standards to the earlier standard wars from the Internet age [9], our data suggests that standardization processes are being shaped by a variety of organizational and environmental characteristics and the previous pattern of standards guiding the nature of interorganizational systems [5] is less evident. Instead, organizational characteristics such as industry and size or geographic boundaries are at least interacting with how the standards themselves will be developed as organizations appear to have flipped the model where use-case brainstorming and proof-of-concepts are also driving the work of consortia in code base and tool development.

Another important aspect relates to our findings on how organizations are adjusting to new governance structures, figuring out IP protecting models, and managing risks of espionage to business competitiveness. It is the well-studied notion in the IS literature that interorganizational systems have consequences for relationship structures between organizations [13, 22] and the reverse, where relationship structures and characteristics such as power differences and network centrality have shaped the nature of interorganizational systems [13]. Our respondents indicated that they are undergoing dramatic mind-shifts in how they approach traditional notions of governance, protection of intellectual property, and espionage risks to competitiveness. In other words, the nature of the blockchain based artifacts indeed suggest that future research must shift focus to new and refined models of relationship structures and configurations of organizations. Models where traditional notions of power, centrality, information asymmetries, trust, structural arrangements and configurations [13], etc. would either play a different role in adoptions of interorganizational systems and in the consequences of adoptions or be replaced with newer notions surrounding distributed power and structural configurations [13], transparency and willingness to share in light of potential information leakages [1], elimination or at least side-tracking of powerful intermediaries; among many others [9, 10]. As Iansiti and Lakhani [9] aptly note, blockchain technologies could stand to deliver on the long awaited and debated changes in the way we regulate and maintain administrative control in the digital age.

## 6. References

[1] I. Adjerid, J. Adler-Milstein, and C. Angst, "Reducing Medicare spending through electronic health

information exchange: the role of incentives and exchange maturity," *Information Systems Research*, 2018.

[2] M. Castillo, *The startup trying to bring blockchain to Wall Street has raised $107 million.* , 2017, http://www.businessinsider.com/r3-consortium-has-raised-107-million-2017-5

[3] Deloitte. "Blockchain technology – the benefits of smart contracts," https://goo.gl/NVGtY9.

[4] K. M. Eisenhardt, and M. E. Graebner, "Theory building from cases: opportunities and challenges," *Academy of management journal*, vol. 50, no. 1, pp. 25-32, 2007.

[5] W. Elgarah, N. Falaleeva, C. C. Saunders, V. Ilie, J. Shim, and J. F. Courtney, "Data exchange in interorganizational relationships: review through multiple conceptual lenses," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, vol. 36, no. 1, pp. 8-29, 2005.

[6] P. Gratzke, D. Schatsky, and E. Piscini, *Banding together for blockchain: Does it make sense for your company to join a consortium?*, 2017, https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/emergence-of-blockchain-consortia.html

[7] E. Griffith, "When the Blockchain Skeptic Walked into the Lion's Den. Available online at: https://www.wired.com/story/when-the-blockchain-skeptic-walked-into-the-lions-den/," *Wired*, 2018.

[8] S. Gupta, and T. Mondal, *HfS Blueprint Report: Enterprise Blockchain Services*, HfS, 2017, https://www.hfsresearch.com/blueprint-reports/hfs-blueprint-enterprise-blockchain-services

[9] M. Iansiti, and K. Lakhani, "The Truth About Blockchain," *Harvard Business Review*, pp. 118-127, 2017.

[10] M. Lacity, *A Manager's Guide to Blockchains for Business*: SB Publishing, 2018.

[11] M. Lacity, K. Moloney, and J. Ross, "Blockchain at BNP Paribas: The Power of Co-Creation," *CISR Case Study*, 2018.

[12] A. Levi, and R. Hackett, *Blockchain in Review: Trends and Opportunities*, CB Insights, 2017, https://www.cbinsights.com/research/briefing/blockchain-trends-and-opportunities/

[13] K. Lyytinen, and J. Damsgaard, "Inter-organizational information systems adoption–a configuration analysis approach," *European journal of information systems*, vol. 20, no. 5, pp. 496-509, 2011.

[14] W. J. Orlikowski, and C. S. Iacono, "Research commentary: Desperately seeking the "IT" in IT research—A call to theorizing the IT artifact," *Information systems research*, vol. 12, no. 2, pp. 121-134, 2001.

[15] L. Orsini, *Personal Interview*, 2017.

[16] L. Orsini, *Industry Impact: Peer-to-Peer Energy Transactions*, Business of Blockchain Conference, Presentation by Principal and Founder, LO3 Energy, 2017, http://events.technologyreview.com/video/watch/lawrence-orsini-lo3-industry-impact/

[17] A. Pazaitis, P. De Filippi, and V. Kostakis, "Blockchain and value systems in the sharing economy: The illustrative case of Backfeed," *Technological Forecasting and Social Change*, vol. 125, 2017.

[18] Quorum, *Quorum White Paper*, JP Morgan Chase, 2016, https://goo.gl/jvzLbH

[19] J. Regenor, "Industry Impact: Aerospace Supply Chain," in Blockchain for Business Conference, MIT, Cambridge Massachusetts, 2017.

[20] J. Regenor, *Personal Interview*, 2018.

[21] *H.R.2810 National Defense Authorization Act* t. U. S. Congress, 2018.

[22] D. Robey, G. Im, and J. D. Wareham, "Theoretical foundations of empirical research on interorganizational systems: assessing past contributions and guiding future directions," *Journal of the Association for Information Systems*, vol. 9, no. 9, pp. 4, 2008.

[23] C. Ross, *Blockchain Brings Us Into The Future, But Only After It Drags Up The Past: Interoperability Becomes An Actual Issue Again*, 2016, http://www.horsesforsources.com/blog/christine-ferrusi-ross/the-interoperability-problems-blockchain-brings_120616

[24] M. D. Seidel, "Questioning Centralized Organizations in a Time of Distributed Trust," *Journal of Management Inquiry*, vol. 27, no. 1, pp. 40-44, 2018.

[25] G. Small, "Additive Manufacturing Reshaping Logistics," 2017.

[26] D. Tapscott, and A. Tapscott, *Blockchain Revolution*, New York City: Penguin, 2016.

[27] The-Linux-Foundation. "The Hyperledger Project Charter," https://www.hyperledger.org/about/charter.